



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002232451 A**(43) Date of publication of application: **16.08.2002**(51) Int. Cl. **H04L 12/46**  
**G06F 13/00**(21) Application number: **2001027120**(22) Date of filing: **02.02.2001**(71) Applicant: **LAYER SEVEN CO LTD**(72) Inventor: **SUGIHARA OSAMU**  
**NAKAZAWA SUSUMU**(54) **COMMUNICATION MANAGEMENT METHOD,  
COMMUNICATION MONITORING SYSTEM,  
AND COMPUTER SYSTEM**

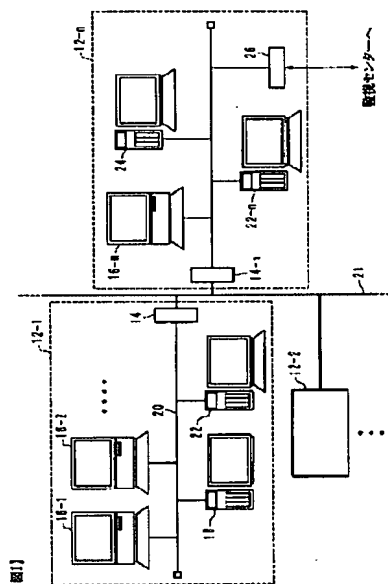
a warning report to the sender via the LAN 20.

COPYRIGHT: (C)2002,JPO

(57) Abstract:

**PROBLEM TO BE SOLVED:** To provide a system that prevents internal data from being leaked or lost to the outside.

**SOLUTION:** A segment controller 22 in a segment demarcated by a router 14 where machines 16, 18 are interconnected via a LAN 20 acquires signal sent onto the LAN 20 and identifies a sender and a transmission destination of the acquired signal. Then the segment controller 22 discriminates whether or not the access right from the sender to the transmission destination exists, the sender is registered and a document going to be sent by the sender is a document whose transmission is inhibited or others. When there exists any trouble, the segment controller 22 requests the machine of the sender and the machine of the destination to disconnect the communication, transmits a report to a system manager to indicate occurrence of an access without the access right for the system manager and/or



(19) 日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11) 特許出願公開番号  
特開2002-232451  
(P2002-232451A)

(43) 公開日 平成14年 8月16日 (2002. 8. 16)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)
H 0 4 L 12/46		H 0 4 L 12/46	M 5 B 0 8 9
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z 5 K 0 3 3
	6 1 0		6 1 0 Q

審査請求 未請求 請求項の数15 O L (全 15 頁)

(21) 出願番号 特願2001-27120(P2001-27120)

(22) 出願日 平成13年 2月 2日 (2001. 2. 2)

(71) 出願人 500093627

レイヤーセブン株式会社

東京都渋谷区渋谷 3-6-2 第二矢木ビル 6 F

(72) 発明者 杉原 修

東京都渋谷区渋谷 3-6-2 第二矢木ビル 6 F レイヤーセブン株式会社内

(72) 発明者 中澤 進

東京都渋谷区渋谷 3-6-2 第二矢木ビル 6 F レイヤーセブン株式会社内

(74) 代理人 100103632

弁理士 壺田 英一郎 (外 1 名)

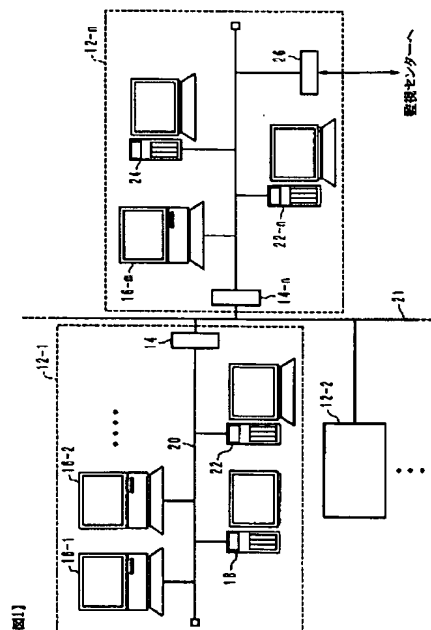
最終頁に続く

(54) 【発明の名称】 通信管理方法、通信監視装置、および、コンピュータシステム

(57) 【要約】

【課題】 内部からのデータの流出や漏洩を防止するためのシステムを提供する。

【解決手段】 ルータ 14 により画定され、かつ、複数のマシン 16、18 が LAN 20 を介して接続されたセグメントにおいて、セグメントコントローラ 22 が、LAN 20 上に送出された信号を取得し、取得した信号の送信元および送信先を特定する。次いで、セグメントコントローラ 22 は、送信元から送信先へのアクセス権の有無や、送信元が登録されているか、送信が禁止されている文書であるか否かなどを判断する。問題がある場合には、送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者にアクセス権の無いアクセスが生じたことを示す、システム管理者にレポートを送信し、および／または、送信元へ LAN 20 を介して警告レポートを送信する。



## 【特許請求の範囲】

【請求項 1】 ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法であって、前記ネットワーク上に送出された信号を取得するステップと、

前記取得した信号の送信元および送信先を特定するステップと、

前記送信元から送信先へのアクセス権の有無を判断するステップと、

前記アクセス権が無い場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者にアクセス権の無いアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成するステップとを備えたことを特徴とする管理方法。

【請求項 2】 送信元のマシンに関する IP アドレスおよびポート番号、送信先のマシンに関する IP アドレスおよびポート番号、並びに、当該送信元から送信先へのアクセスの際に実行すべき処置からなるデータの組をデータベース中に記憶するステップを備え、

前記アクセス権の有無を判断するステップが、データベースを検索して、送信元のマシンに関する処置を特定することにより、必要な処置を決定することを特徴とする請求項 1 に記載の管理方法。

【請求項 3】 ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法であって、

前記ネットワークに接続されたマシンの MAC アドレスを登録するステップと、

前記ネットワーク上に送出された信号を取得するステップと、

前記取得した信号の送信元および送信先を特定するステップと、

前記送信元の MAC アドレスが登録されているか否かを判断するステップと、

前記 MAC アドレスが登録されていない場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者に登録のないマシンによるアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成するステップとを備えたことを特徴とする管理方法。

【請求項 4】 ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法であって、

前記ネットワーク上に送出された信号を取得するステップと、

前記取得した信号がメール送信であることを判断するステップと、

前記メール送信が認められるものであるか否かを判断するステップと、

前記メール送信が認められないものである場合に、メールサーバに対して、メール送信の中止を要求し、認められないメール送信が生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成するステップとを備えたことを特徴とする管理方法。

【請求項 5】 前記メール送信が認められるものであるか否かを判断するステップが、

前記信号を走査して、送信が禁止されている宛て先ではないこと、添付ファイルの有無、および／または、文字列中に禁止されたものが含まれないことを判断することを特徴とする請求項 4 に記載の管理方法。

【請求項 6】 ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法であって、

前記ネットワーク上に送出された信号を取得するステップと、

前記取得した信号の送信元および送信先を特定するステップと、

前記信号を解析して、当該信号に基づく文字列に禁止されたものが含まれているか否かを判断するステップと、

前記信号に基づく文字列が含まれている場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者にアクセス権の無いアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成するステップとを備えたことを特徴とする管理方法。

【請求項 7】 ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法であって、

各マシンに、所定期間におけるユーザによる少なくともキー入力を蓄積するエージェントプログラムをインストールするステップと、

前記エージェントプログラムにより所定のタイミングにて、蓄積されたキー入力を示す情報を受理して、これを解析するステップと、

前記解析の結果、キー入力による文字列中に禁止されているものが含まれている場合に、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成

するステップとを備えたことを特徴とする管理方法。

【請求項 8】 前記システムが、1 以上のルータにより画定されたセグメントであって、当該セグメント中に 1 以上のマシンが配置されたセグメントを有し、各セグメントにおいて、ネットワーク上に送出された信号に基づき、前記ステップが実行されることを特徴とする請求項 1 ないし 7 の何れか一項に記載の管理方法。

【請求項 9】 ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を監視する通信監視装置であって、前記ネットワーク上に送出された信号を取得する信号取得手段と、

前記取得した信号の送信元および送信先を特定する通信マシン特定手段と、

前記送信元から送信先へのアクセス権の有無を判断するアクセス権判断手段と、

前記アクセス権が無い場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者にアクセス権の無いアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成する処置手段とを備えたことを特徴とする通信監視装置。

【請求項 10】 さらに、送信元のマシンに関する IP アドレスおよびポート番号、送信先のマシンに関する IP アドレスおよびポート番号、並びに、当該送信元から送信先へのアクセスの際に実行すべき処置からなるデータの組を記憶したデータベースを備え、前記アクセス権判断手段が、前記データベースを検索して、送信元のマシンに関する処置を特定することにより、必要な処置を決定することを特徴とする請求項 9 に記載の通信監視装置。

【請求項 11】 ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を監視する通信監視装置であって、前記ネットワークに接続されたマシンの MAC アドレスを登録するマシン登録手段と、

前記ネットワーク上に送出された信号を取得する信号取得手段と、

前記取得した信号の送信元および送信先を特定する通信マシン特定手段と、

前記送信元の MAC アドレスが既に登録されているか否かを判断する公式マシン判断手段と、

前記 MAC アドレスが登録されていない場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者に登録のないマシンによるアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へ

ネットワークを介して伝達すべき警告レポートを作成する処置手段とを備えたことを特徴とする通信監視装置。

【請求項 12】 ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を監視する通信監視装置であって、前記ネットワーク上に送出された信号を取得する信号取得手段と、

前記取得した信号がメール送信であることを判断して、当該メール送信が認められるものであるか否かを判断するメール送信特定手段と、

前記メール送信が認められないものである場合に、メールサーバに対して、メール送信の中止を要求し、認められないメール送信が生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成する処置手段とを備えたことを特徴とする通信監視装置。

【請求項 13】 ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を監視する通信監視装置であって、前記ネットワーク上に送出された信号を取得する信号取得手段と、

前記取得した信号の送信元および送信先を特定する通信マシン特定手段と、

前記信号を解析して、当該信号に基づく文字列が送信を禁止されたものであるか否かを判断する信号解析手段と、

前記文字列が送信を禁止されたものである場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者にアクセス権の無いアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成する処置手段とを備えたことを特徴とする通信監視装置。

【請求項 14】 ルータに画定されたセグメントであって、当該セグメント中に 1 以上のマシンが配置された、1 以上のセグメントを有し、各セグメントが、請求項 9 ないし 13 の何れか一項に記載の通信監視装置を有することを特徴とするコンピュータシステム。

【請求項 15】 各通信監視装置が、セグメント内のマシン間の通信制限に関する固有の情報と、セグメント間および外部との通信制限に関する共通の情報とを記憶したデータベースを有することを特徴とする請求項 14 に記載のコンピュータシステム。

【発明の詳細な説明】

【0001】

【産業上の技術分野】 本発明は、社内からの情報の流出や漏洩を防止するシステムに関する。

## 【0002】

【従来の技術】企業や組織内においては、LANなどのネットワークによりコンピュータ（クライアントマシン）やサーバが相互に接続され、データの共有、ユーザ間のメール通信などが行われている。また、インターネットの著しい普及により、ルータおよびインターネットを介して、社内のマシンと外部のサーバ等が接続される状態となっている場合が多い。

【0003】このように内部における相互のデータ通信や外部と内部の間のデータ通信が可能となると、外部からの侵入を防止するとともに、内部からのデータ流出や漏洩を防止することが重要となる。たとえば、インターネットを介した外部からの侵入に対してはファイアウォールを設けることである程度防止できる。したがって、企業や組織内に構築されたコンピュータシステムにおいては、外部との境界に、グローバルIP領域（外部）とローカルIP領域（内部）とを画定するファイアウォールを設けている。

## 【0004】

【発明が解決しようとする課題】ところが、ファイアウォールでは、内部からの漏洩や流出を防止することができない。実際に、不正アクセスは、外部からの侵入よりも内部からの流出が多いのが現状である。故意にデータを持ち出すほか、不注意なメール送信等もしばしば起こり得る。さらに、LANなど内部のネットワークに、従業者等が自身のマシンを接続することにより、当該マシンが感染しているウィルスに、内部のクライアントマシン全体が感染するというおそれもある。本発明は、内部からのデータの流出や漏洩を防止するためのシステムを提供することを目的とする。

## 【0005】

【課題を解決するための手段】本発明の目的は、ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法であって、前記ネットワーク上に送出された信号を取得するステップと、前記取得した信号の送信元および送信先を特定するステップと、前記送信元から送信先へのアクセス権の有無を判断するステップと、前記アクセス権が無い場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者にアクセス権の無いアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成するステップとを備えたことを特徴とする管理方法により達成される。

【0006】本発明によれば、ローカルなネットワークを介して複数のマシンが接続されたシステムにおいて、当該ネットワーク上に送出される信号（パケット）を取得し、当該パケットに基づき、送信元および送信元を特

定し、アクセス権の有無を判断している。また、アクセス権が存在しない場合には、たとえば、送信元および送信先の双方に対して、通信切断を要求する。したがって、故意或いは不注意による不正なアクセスを防止し、或いは、これを送信元や管理者に通知することが可能となる。

【0007】本発明の好ましい実施態様においては、送信元のマシンに関するIPアドレスおよびポート番号、送信先のマシンに関するIPアドレスおよびポート番号、並びに、当該送信元から送信先へのアクセスの際に実行すべき処置からなるデータの組をデータベース中に記憶するステップを備え、アクセス権の有無を判断するステップが、データベースを検索して、送信元のマシンに関する処置を特定することにより、必要な処置を決定するように構成されている。この実施態様によれば、データの組を変更し、或いは、追加することにより、アクセス権の変化に柔軟に対応することが可能となる。

【0008】本発明の別の実施態様において、ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法は、前記ネットワークに接続されたマシンのMACアドレスを登録するステップと、前記ネットワーク上に送出された信号を取得するステップと、前記取得した信号の送信元および送信先を特定するステップと、前記送信元のMACアドレスが登録されているか否かを判断するステップと、前記MACアドレスが登録されていない場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者に登録のないマシンによるアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成するステップとを備えている。この実施態様によれば、ローカルなネットワークに接続可能なマシンを予め登録し、登録されたマシン（公式マシン）のみがネットワークを介したアクセスを認めることが可能となる。

【0009】本発明のさらに別の実施態様において、ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法は、ネットワーク上に送出された信号を取得するステップと、取得した信号がメール送信であることを判断するステップと、メール送信が認められるものであるか否かを判断するステップと、メール送信が認められないものである場合に、メールサーバに対して、メール送信の中止を要求し、認められないメール送信が生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成するステップ

とを備えている。これにより、認められないメール送信を防止すること、或いは、メールが既に送信されてしまった場合であっても、これを管理者や送信元に知らせることが可能となる。

【0010】より好ましい実施態様においては、メール送信が認められるものであるか否かを判断するステップが、信号を走査して、禁止された送信先であること、添付ファイルの有無、および／または、文字列中に禁止されたものが含まれないことを判断する。

【0011】別の実施態様において、ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法は、ネットワーク上に送出された信号を取得するステップと、取得した信号の送信元および送信先を特定するステップと、信号を解析して、当該信号に基づく文字列に禁止されたものが含まれているか否かを判断するステップと、信号に基づく文字列が含まれている場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者にアクセス権の無いアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成するステップとを備えている。

【0012】本発明のさらに別の実施態様において、ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を管理する管理方法は、各マシンに、所定期間におけるユーザによる少なくともキー入力を蓄積するエージェントプログラムをインストールするステップと、エージェントプログラムにより所定のタイミングにて、蓄積されたキー入力を示す情報を受理して、これを解析するステップと、解析の結果、キー入力による文字列中に禁止されているものが含まれている場合に、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成するステップとを備えている。暗号化されたメール送信においては、ネットワークに送出されたパケットからは容易に、送信文中に問題のある文字列が含まれるか否かを判断することができない。そこで、この実施態様においては、キー入力を蓄積しておき、蓄積されたキー入力を解析して、問題のある文字列が存在したか否かを判断し、存在する場合には、これを管理者等に通知している。これにより、メール送信自体を防止できないものの、不正なメール送信が生じた可能性があること自体を知ることが可能となる。

【0013】システムは、1以上のルータにより画定されたセグメントであって、当該セグメント中に1以上のマシンが配置されたセグメントを有し、各セグメントに

において、ネットワーク上に送出された信号に基づき、前記ステップが実行されても良い。

【0014】また、本発明の目的は、ルータにより外部との間が画定され、かつ、複数のマシンがローカルなネットワークを介して接続されたシステムにおいて、マシン間およびマシンから外部への通信を監視する通信監視装置であって、前記ネットワーク上に送出された信号を取得する信号取得手段と、前記取得した信号の送信元および送信先を特定する通信マシン特定手段と、前記送信元から送信先へのアクセス権の有無を判断するアクセス権判断手段と、前記アクセス権が無い場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者にアクセス権の無いアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成する処置手段とを備えたことを特徴とする通信監視装置によっても達成される。

【0015】別の実施態様において、通信監視装置は、ネットワークに接続されたマシンのMACアドレスを登録するマシン登録手段と、ネットワーク上に送出された信号を取得する信号取得手段と、取得した信号の送信元および送信先を特定する通信マシン特定手段と、送信元のMACアドレスが既に登録されているか否かを判断する公式マシン判断手段と、MACアドレスが登録されていない場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者に登録のないマシンによるアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成する処置手段とを備えている。

【0016】また、別の実施態様において、通信管理装置は、前記ネットワーク上に送出された信号を取得する信号取得手段と、前記取得した信号の送信元および送信先を特定する通信マシン特定手段と、前記信号を解析して、当該信号に基づく文字列が送信を禁止されたものであるか否かを判断する信号解析手段と、前記文字列が送信を禁止されたものである場合に、前記送信元のマシンおよび送信先のマシンに対して、通信の切断を要求し、システム管理者にアクセス権の無いアクセスが生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成する処置手段とを備えている。

【0017】さらに別の実施態様において、通信監視装置は、前記ネットワーク上に送出された信号を取得する信号取得手段と、前記取得した信号がメール送信であることを判断して、当該メール送信が認められるものであるか否かを判断するメール送信特定手段と、前記メール送信が認められないものである場合に、メールサーバに

対して、メール送信の中止を要求し、認められないメール送信が生じたことを示す、システム管理者に伝達すべきレポートを作成し、および／または、前記送信元へネットワークを介して伝達すべき警告レポートを作成する処置手段とを備えている。

【0018】上記通信監視装置は、ルータに画定されたセグメントであって、当該セグメント中に1以上のマシンが配置された、1以上のセグメントの各々に配置されていても良い。この場合には、各通信監視装置が、セグメント内のマシン間の通信制限に関する固有の情報と、セグメント間および外部との通信制限に関する共通の情報とを記憶したデータベースを有するのが望ましい。

【0019】

【発明の実施の形態】以下、添付図面を参照して、本発明の実施の形態につき説明を加える。図1は、本発明の実施の形態にかかるシステムの全体を示すブロックダイヤグラムである。この実施の形態においては、ある企業や組織内のシステム（社内システム）における内部からの情報流出を防止するために本発明を適用している。図1に示すように、この社内システムは、複数のセグメント12-1、12-2、・・・を有している。各セグメント（たとえばセグメント12-1）においては、ルータ14、クライアントマシン16-1、16-2、・・・、サーバ18等が設けられている。クライアントマシンおよびサーバは、セグメント内のLAN20にて相互に接続されている。また、LAN20に接続されたルータを介して他のセグメントや外部とのデータ通信も可能である。

【0020】また、各セグメント12には、セグメント内の通信状況を監視し、必要な場合にデータ通信の終了（マシン間の切断）などの処理を実行するセグメントコントローラ22が設けられている。セグメントコントローラ22は、主として、設置されたセグメント12において、LAN20上で伝達されるデータ（パケット）を監視するようになっている。各セグメント12-1、12-2、・・・はLAN21を介して接続され、相互にデータ通信をなすことができる。

【0021】また、あるセグメント12-nには、クライアントマシン16-mなどや、セグメントコントローラ22-nのほか、社内システムや、他の社内システム（図示せず）など、監視対象となるシステム全体を中央で監視する監視センターとのデータ送受信を制御する監視コンソール24や外部ネットワーク（たとえばインターネット）との境界に配置されたルータ26が設けられている。

【0022】図2は、セグメントコントローラ22の構成を示すブロックダイヤグラムである。図2に示すように、セグメントコントローラ22は、LAN20上の信号（パケット）を取り入れて信号を監視する通信監視部32と、通信監視部32により取り込まれた信号に基づ

き、クライアントマシン間、クライアントマシンとサーバとの間などのアクセス権の有無を判断するアクセス権管理部34と、アクセス権等に関する種々の情報を記憶したアクセス権データベース（DB）36と、LAN20上に信号を送出したマシンを特定するマシン特定部38と、LAN20上に送出された信号に基づき、送信先のアドレスや信号中に含まれる文字列を特定する文字列／アドレス特定部40と、送信を制限すべき送信先や通信文中の文字列が記憶された送信制限情報DB42と、後述するクライアントマシン中のエージェントプログラムから、クライアントマシンへのユーザによるキー入力を示すデータを受理するキー入力受理部44と、ユーザによるキー入力記憶されたキー入力DB46と、キー入力を解析するキー入力解析部48と、必要な場合に、アクセスが行われようとしているマシン間に通信切断を求める通信切断処理部50と、不正なアクセスなどを管理者等に通知するための処理を実行する警告処理部52と、アクセスログを記憶するアクセスログDB54とを有している。

【0023】このように構成されたセグメントコントローラを利用して、本実施の形態においては、以下のような監視が実現される。

- (1) アクセス制限の設定、アクセス権を伴わないアクセスの禁止、通知
  - (2) 非公式PC（登録されていないPC）のネット上での接続禁止
  - (3) 不要なメール送信の遮断
  - (4) キー入力のモニターおよび解析
- これらにつき、以下に説明を加える。

【0024】(1) アクセス制限の設定等

図3および図4は、本実施の形態にかかるアクセス制限に関する処理手順を示すフローチャートである。なお、ここでは、あるクライアントマシン16が、同一のセグメント12内のサーバ18にアクセスする場合につき説明を加えるが、これに限定されるものではなく、クライアントマシン間のアクセスやセグメント外の各マシンへのアクセスについても同様の処理が実行される。

【0025】図3に示すように、クライアントマシン16（この場合にはクライアントマシン「a」16-1）から、サーバ18（この場合にはサーバ「A」18-1）に、アクセス要求がLAN20を介して送信された際に（ステップ301）、セグメントコントローラ22の通信監視部32は、LAN20上に送出されたこのアクセス要求を取得し（ステップ301-b）、アクセス元およびアクセス先のマシンを特定する（ステップ302）。次いで、アクセス権管理部34は、アクセス権DB36を参照して、アクセス元からアクセス先へのアクセス権があるか否かを判断する（ステップ303）。アクセス権がある場合には、セグメントコントローラ22は、アクセス元からアクセス先へのアクセスがあったこ

と、および、その日時を含むアクセスログを作成し、これをアクセスログDB54に記憶する(ステップ304)。この場合には、アクセス先であるサーバ「A」18-1は、アクセスに応答した処理を実行して(ステップ305)、必要なデータなどを含む応答をクライアントマシン「a」16-1に返送する(ステップ306)。

【0026】その一方、アクセス権がなかった場合につき図4を参照して説明を加える。ここでは、クライアントマシン16(クライアントマシン「a」16-1)が、アクセス権限のないサーバ18(この場合にはサーバ「B」18-2)にアクセス要求をした場合について説明する。

【0027】図4においてステップ401～ステップ403は、図3のステップ301～ステップ303と同じである。アクセス権がないと判断された場合には(ステップ403参照)、セグメントコントローラ22の通信切断処理部50が、アクセス元のマシン(クライアントマシン「a」16-1)およびアクセス先のマシン(サーバ「B」18-2)の双方に、通信切断要求を送信する(ステップ404、405)。この通信切断要求は、アクセス先のマシンにとってはアクセス元からの切断要求と解釈され、アクセス元のマシンにとってはアクセス先からの切断要求と解釈されるようなものであるのが望ましい。

【0028】これにより、クライアントマシン「a」16-1およびサーバ「B」18-2において通信切断の処理が実行される(ステップ407、408)。これにより、アクセス権のないマシンからのアクセスが阻止される。次いで、アクセスログがアクセスログDB54に記憶される(ステップ408)。また、必要に応じて、アクセス権の無いマシンからのアクセスがあったことを示す通知レポートやアクセス権の無いマシンに対するアクセスが認められなかったことを示す警告レポートが、警告通知処理部52にて作成され、これが送信される(ステップ409)。たとえば、通知レポートは、監視コンソール24に送信されれば良い。また、警告レポートはアクセス権のないアクセス先へのアクセス要求をしたマシンに送信される。

【0029】図5は、本実施の形態におけるアクセス権DB36に記憶されたデータの例を示す図である。図5に示すように、アクセス権DB36においては、セグメント12内のマシン間に関するアクセス権を規定したアクセス権情報500と、セグメント内外を含むシステム内のアクセス権を規定したシステム内アクセス権情報510とが設けられている。セグメント内アクセス権情報500は、各セグメント12に固有のものであり、各セグメント内に配置されたセグメントコントローラ22がそれぞれ保有している。その一方、システム内アクセス権情報510は、全てのセグメントコントローラ22が共

通して保有している。

【0030】たとえば、セグメント内アクセス権情報500は、ソースマシン(アクセス元)のIPアドレスやポート番号からなるソースマシン情報(符号501参照)と、宛て先マシン(アクセス先)のIPアドレスやポート番号からなる宛て先マシン情報(符号502参照)と、ソースマシンから宛て先マシンへのアクセス制限の内容を示す制限情報(符号503参照)とからなるデータの組を含んでいる。アクセス制限には、たとえば、通信の切断、管理者やアクセス元ユーザへの通知、および/または、ログの記録が含まれる。アクセス権DB36は、必要な組み合わせのデータの組を収容している。これは、必要に応じて、アクセス権管理部34により更新され得る。

【0031】また、システム内アクセス権情報510も、セグメント内アクセス権情報500のデータの組と同様の構成を有するものを含んでいる。したがって、これを参照することにより、セグメント外へのアクセスや、たとえばインターネットを介するシステム外へのアクセスに関するアクセス権の有無を判断することもできる。

【0032】アクセス権の有無を判断する処理(図3のステップ303、図4のステップ403)においては、アクセス権管理部34が、アクセス権DB36を検索して、当該ソースマシン(アクセス元)に関して、宛て先マシンおよびアクセス制限がどのようになっているかを特定すれば良い。

【0033】このように、本実施の形態においては、セグメント内のアクセス、セグメント間のアクセス、さらには、システム外へのアクセスについて、セグメントコントローラがセグメント中のLAN上を通る信号を監視し、必要な場合には、アクセス制限にしたがって、通信の切断などの処理を実行する。したがって、認められないアクセスを防止することが可能となる。

【0034】(2)非公式PCのアクセス禁止

また、本実施の形態においては、予め登録されたマシン以外のマシンによる他のマシンへのアクセスを禁止できるようになっている。たとえば、ユーザが個人のマシンを持参してLAN20に接続する場合がある。このようなときに、個人のマシンがウィルスに感染していたり、何らかのトラブルが生じていると、当該個人のマシンによるアクセスによって、他のマシンにも障害が生じるおそれがある。また、個人のマシンに情報がダウンロードされることにより、社外秘など秘密保持すべき情報が外に持ち出されるおそれもある。本実施の形態においては、このようなアクセスを制限し、他のマシンへの障害や情報の持ち出し等を適切に防止する。

【0035】このために、セグメントコントローラ22は、たとえば、セグメント12中に配置されLAN20と接続されているクライアントマシン16やサーバ18の、それぞれのMACアドレスをアクセス権DB36に



記憶しておくのが望ましい。図6は、予め登録されていないクライアントマシン（非公式クライアントマシン）によるアクセスの際に実行される処理を示すフローチャートである。図6に示すように、非公式クライアントマシンから、たとえば、あるサーバ18（この場合にはサーバ「A」18-1）に、アクセス要求がLAN20を介して送信された際に（ステップ601）、セグメントコントローラ22の通信管理部32は、LAN20上に送出されたこのアクセス要求を取得する（ステップ601-b）。

【0036】次いで、マシン特定部38は、アクセス元のMACアドレスを特定し、アクセス権DB36を検索して、当該MACアドレスが登録されているものか否か、つまり、アクセス元が公式マシンか否かを判断する（ステップ602）。MACアドレスが登録されている場合には（ステップ602でイエス(Yes)）、図3のステップ304と略同様の処理が実行される。その一方、ステップ602にてノー(No)と判断された場合には、アクセス元である非公式クライアントマシンおよびアクセス先のマシン（サーバ「A」18-1）の双方に、通信切断要求を送信する（ステップ603、604）。これにより、非公式クライアントマシンおよびサーバ「B」18-2において通信切断の処理が実行される（ステップ605、606）。これにより、非公式マシンからのアクセスが阻止される。

【0037】次いで、アクセスログがアクセスログDB54に記憶される（ステップ607）。また、必要に応じて、非公式マシンからのアクセスがあったことを示す通知レポートや非公式マシンに対するアクセスが認められなかったことを示す警告レポートが、警告通知処理部52にて作成され、これが送信される（ステップ608）。

#### 【0038】（3）不要なメール送信の遮断

さらに、本実施の形態においては、認められていないメール送信を阻止するための処理を実行することもできる。これは、LAN上に送出されたメールを監視することにより実現される。図7は、メール送信の遮断処理を示すフローチャートである。図7に示すように、あるクライアントマシン（この場合にはクライアントマシン「a」16-1）からメール（メールのバケット）が送信されたときに、セグメントコントローラ22の通信管理部32は、LAN20上に送出されたメールのバケットを取得し（ステップ701-b）、文字列／アドレス特定部40が、当該メールがメールサーバを介して送信先に送信すべきものであるか否かを判断する（ステップ702）。

【0039】図8は、本実施の形態におけるステップ702のメール送信許可判断処理を示すフローチャートである。図8に示すように、セグメントコントローラ22の文字列／アドレス特定部40は、まず、メールの送信

元および送信先を特定する（ステップ801）。本実施の形態においては、送信制限情報DB42に、送信先の制限に関する情報、添付ファイルの送信の認否などを示す情報が記憶されている。たとえば、マシンごとにメール送信先の制限、添付ファイルの認否が設定され、その情報が記憶されていても良い。たとえば、これにより、マシンごとに事前に登録した送信先以外のメール送信を禁止し、或いは、所定の送信先に宛てたメール送信を禁止することができる。或いは、一括して送信が認められないメール送信先が設定され、或いは、添付ファイルが認められないことなどが設定あせれていても良い。

【0040】さらに、本実施の形態においては、メールの送信文を走査して、認められていない文字列を検出することができるようになっている。文字列／アドレス特定部40は、送信元のマシンが特定されると、送信が認められたメールの送信先であるか否か（ステップ802）、添付ファイルの有無（ステップ803）および禁止された文字列が送信文中に含まれるか否か（ステップ804）を判断し、これらの条件が合致する場合（全てのステップでノー(No)）の場合に、メール送信を許可する（ステップ702にてイエス(Yes)）。メール送信が認められる場合には、図3のステップ304以降の処理が実行される。

【0041】その一方、ステップ802～804の何れかにおいてイエス(Yes)と判断されると、送信を許可すべきでないと判断され（ステップ702にてノー(No)）、その結果、メール不送信要求が作成され（ステップ805）、これがメールサーバに送信される（ステップ703）。これにより、メールサーバにおいては、メール送信が中止される（ステップ704）。

【0042】また、アクセスログがアクセスログDB54に記憶され（ステップ705）、かつ、送信が認められていない送信先等へのメール送信があったことを示す通知レポートや、送信元のマシンに対する警告レポートが、警告通知処理部52にて作成され、これが、それぞれ管理者や送信元のマシンに向けて送信される（ステップ706）。たとえば、短い送信文の場合には、メールサーバを介して既に送信先に送信されてしまっている可能性もある。したがって、ここでは通知レポートの作成および管理者への通知が行われることが望ましい。

【0043】（4）キー入力モニターおよび解析  
上述したように、本実施の形態では、メール送信文に含まれる文字列を走査して、禁止された文字列が含まれているか否かが判断される。しかしながら、メール本文を暗号化して送信する場合については、これを復号して、問題のあるメール送信を阻止することは困難である。そこで、本実施の形態においては、クライアントマシン16の各々にエージェントプログラムを予めインストールして、エージェントプログラムが、ユーザのキーストロークを蓄積している。蓄積されたキーストロークのデー

タは、セグメントコントローラ22において解析され、問題のある入力があるか否かが調べられる。これにより、事後的ではあるが、秘密保持すべき情報の漏洩があったか否かなどを知ることが可能となる。

【0044】図9は、本実施の形態にかかるキーストローク解析の処理を示すフローチャートである。クライアントマシン16のエージェントプログラムは、ユーザのキーストロークを蓄積する(ステップ901)。所定の期間(たとえば1日)だけ蓄積されたキーストローク情報は、所定のタイミングで、当該クライアントマシン16が配置されたセグメント12中のセグメントコントローラ22に伝達される(ステップ902)。

【0045】セグメントコントローラ22がキーストローク情報を受理すると、キー入力受理部44が、これをユーザと関連付けてキー入力DB46に記憶する(ステップ403)。次いで、キー入力解析部48は、キー入力DB46中のキーストローク情報を読み出して、これを解析する(ステップ904)。この解析においては、たとえば、押下されたキーの組み合わせから、禁止された文字列が含まれるか否かなどが判断される(ステップ905)。キーストロークに基づく解析の結果、何らかの問題が生じている場合には(ステップ905でイエス(Yes))、監視コンソール24の管理者に向けて、通知レポートを作成して送信する(ステップ906)。この通知レポートにおいては、クライアントマシン名、ユーザ名、解析の結果生じていたと考えられる問題点が記述されれば良い。これにより、事後的に、クライアントマシンのユーザによる問題のあるキー入力を知ることができる。

【0046】本実施の形態にかかる監視コンソール24においては、セグメントコントローラ22からの通知レポート等を受理して、これを表示装置の画面上に表示できるようにしている。図10は、監視コンソール24の表示装置の画面上に表示された画像例を示す図である。図10(a)に示すように、監視コンソール24の表示装置の画面上には、システム中のマシン(クライアントマシン16、サーバ18など)およびLANの接続形態が表示される。図10(a)において、たとえば、符号1002にて示すものがマシンを表し、符号1003にて示すものがLANを表す。ここで、セグメントコントローラ22により、あるセグメント中のマシンにおいて、(1)~(4)にて説明した問題(アクセス権の無いマシンへのアクセス、非公式マシンによるアクセス、禁止されたメール送信、キー入力における問題)が生じていると判断され、通知レポートが、監視コンソール24に与えられた場合には、当該問題が生じたマシンが、たとえば、点滅するなど他のマシンと区別して表示される(符号1004参照)。

【0047】監視コンソール24の操作者(管理者)は、マウスなどの入力装置を操作して、図10(a)の

画像中の問題が生じたマシンを指定することにより、図10(b)に示すように、通知レポートに含まれた情報から生成された画像を表示装置の画面上に表示させることができる。この画像には、たとえば、マシン名、ユーザ名、問題が発生した日時、その種別および内容、並びに、問題に対する処置が含まれる。これにより、管理者は、システム中のどのマシンに問題が生じているかをリアルタイムに把握することができる。

【0048】また、入力装置を操作してマシンを指定して、ログの表示コマンドを入力することにより、当該マシンのログを表示することができる。このログは、マシンが配置されたセグメント中のセグメントコントローラから、必要に応じて送信されても良い。或いは、セグメントコントローラが所定のタイミングで、セグメント中のマシンのログを監視コンソールに伝達し、これを監視コンソールがDB中に記憶しておき、必要に応じて、DBを読み出すように構成しても良い。

【0049】さらに、監視コンソール24は、外部ネットワークを介して、監視センターに必要なレポート(たとえば月次レポート)を送信することもできる。また、特に必要な場合(単に、問題のあるアクセスを検出するだけでなく、何らかの特別な対策を講じるべき場合など)には、監視センターに、問題のあるアクセスに関するレポートを送信して、対応策を仰ぐことも可能である。

【0050】本発明は、以上の実施の形態に限定されることなく、特許請求の範囲に記載された発明の範囲内で、種々の変更が可能であり、それらも本発明の範囲内に包含されるものであることは言うまでもない。たとえば、前記実施の形態においては、システム内を複数のセグメントに分割し、セグメントごとにセグメントコントローラを配置し、基本的に、セグメント内のマシンのアクセスに関してはセグメントコントローラが監視および必要な処置を施すように構成しているが、これに限定されるものではなく、システム内を単一のセグメントから構成し、これを単一のセグメントコントローラがマシンを監視等するようにしても良い。なお、この場合には、セグメントコントローラおよび監視コンソールを一体として形成するのが望ましい。

【0051】また、前記実施の形態において、何らかの問題のあるアクセス(アクセス権の無いアクセス、非公式マシンによるアクセス、問題のあるメール送信)について、通信切断および通知レポートの作成の処理を実行しているが、これに限定されるものではない。これら処置は、マシンごと、IPアドレスごとに、必要な処置を設定しておき、設定された条件にしたがって、必要な処理を実行すればよい。

【0052】さらに、前記実施の形態において、文字列/アドレス特定部40は、メール送信にかかる信号を解析して、当該信号により特定される文字列にて禁止され

ているものが含まれているか否かを判断しているが、これに限定されるものではない。たとえば、LAN上に送出されたパケットを取得し、これらのパケット中に禁止された文字列が含まれるか否かを判断するように構成しても良い。すなわち、WEB閲覧、FTPによるファイル転送、TELNETなどの全ての操作に対して、当該操作やそのための文字列をモニターして、禁止された操作や文字列の送信を防止することも可能である。なお、本明細書において、一つの手段の機能が、二つ以上の物理的手段により実現されても、若しくは、二つ以上の手段の機能が、一つの物理的手段により実現されてもよい。

【0053】

【発明の効果】本発明によれば、内部からのデータの流出や漏洩を防止するためのシステムを提供することが可能となる。

【図面の簡単な説明】

【図1】 図1は、本発明の実施の形態にかかるシステムの全体を示すブロックダイアグラムである。

【図2】 図2は、本実施の形態にかかるセグメントコントローラの構成を示すブロックダイアグラムである。

【図3】 図3は、本実施の形態にかかるアクセス制限に関する処理手順を示すフローチャートである。

【図4】 図4は、本実施の形態にかかるアクセス制限に関する処理手順を示すフローチャートである。

【図5】 図5は、本実施の形態におけるアクセス権DBに記憶されたデータの例を示す図である。

【図6】 図6は、本実施の形態において、非公式クライアントマシンによるアクセスの際に実行される処理を\*

\*示すフローチャートである。

【図7】 図7は、本実施の形態にかかるメール送信の遮断処理を示すフローチャートである。

【図8】 図8は、本実施の形態におけるメール送信許可判断処理を示すフローチャートである。

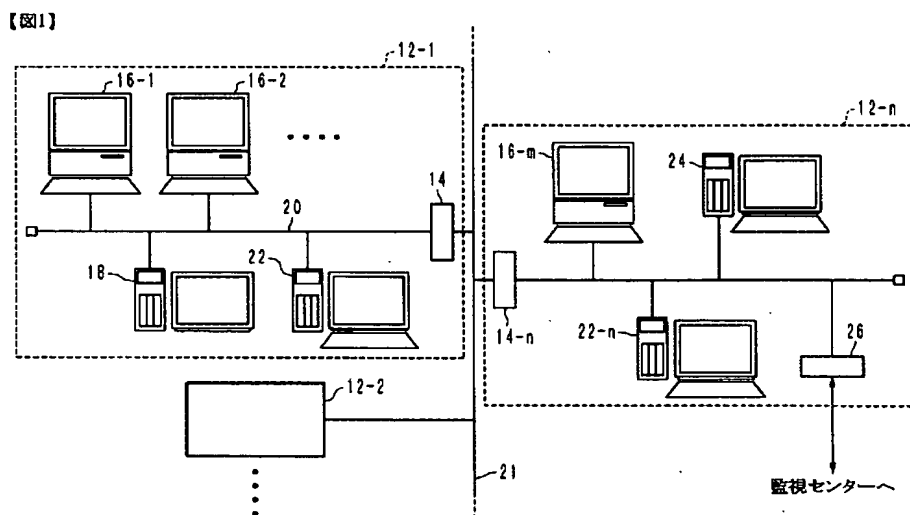
【図9】 図9は、本実施の形態にかかるキーストローク解析の処理を示すフローチャートである。

【図10】 図10は、本実施の形態にかかる監視コンソールの表示装置の画面上に表示された画像例を示す図である。

【符号の説明】

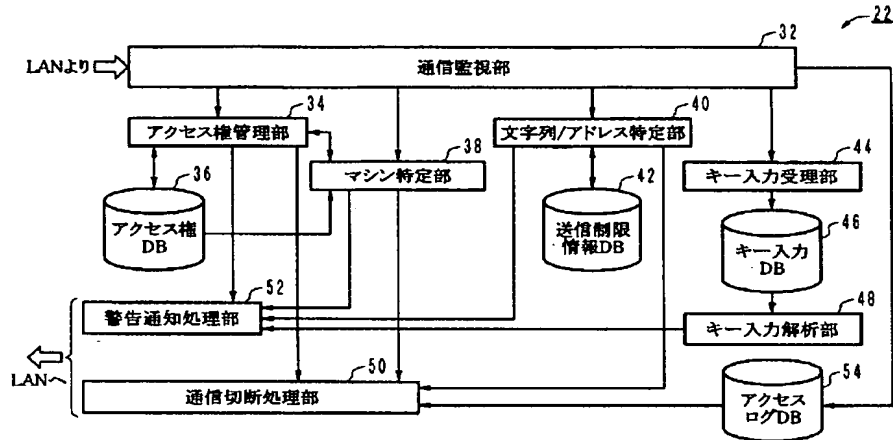
12	セグメント
14	ルータ
16	クライアントマシン
18	サーバ
20	LAN
22	セグメントコントローラ
24	監視コンソール
32	通信管理部
34	アクセス権管理部
36	アクセス権DB
38	マシン特定部
40	文字列／アドレス特定部
42	送信制限情報DB
44	キー入力受理部
46	キー入力DB
48	キー入力解析部
50	通信切断処理部
52	警告通信処理部

【図1】



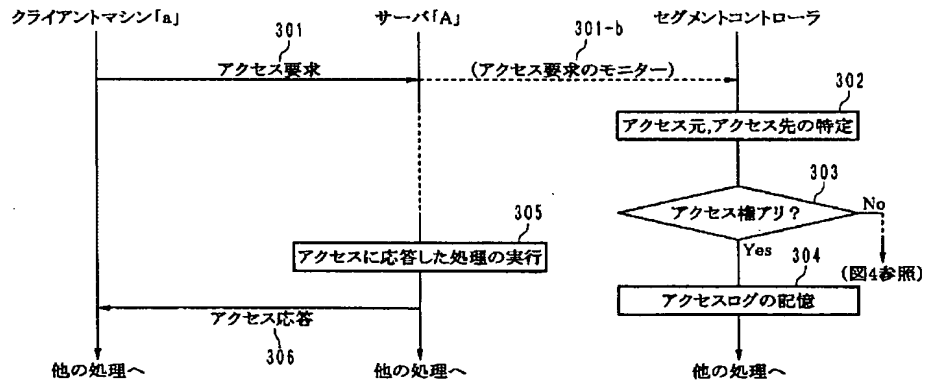
【図2】

【図2】



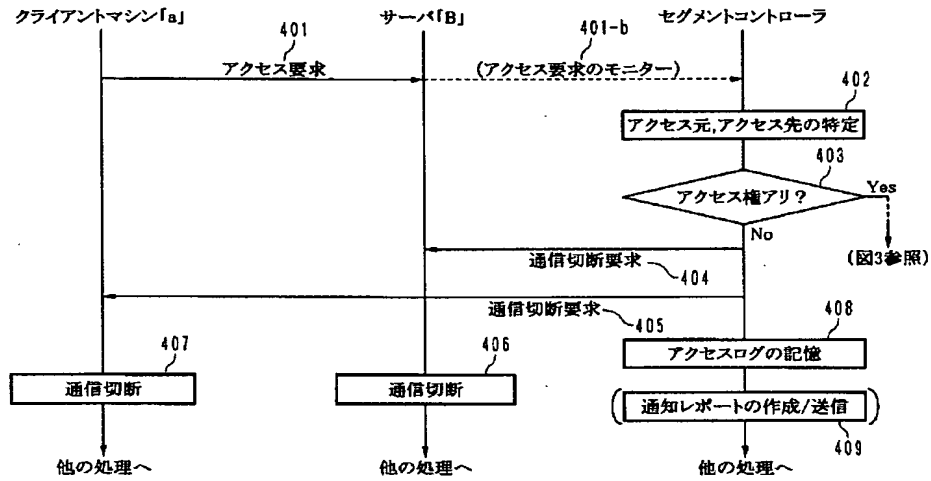
【図3】

【図3】



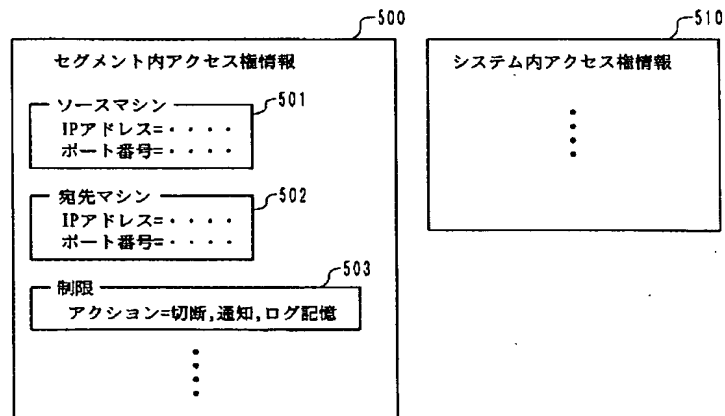
【図4】

【図4】



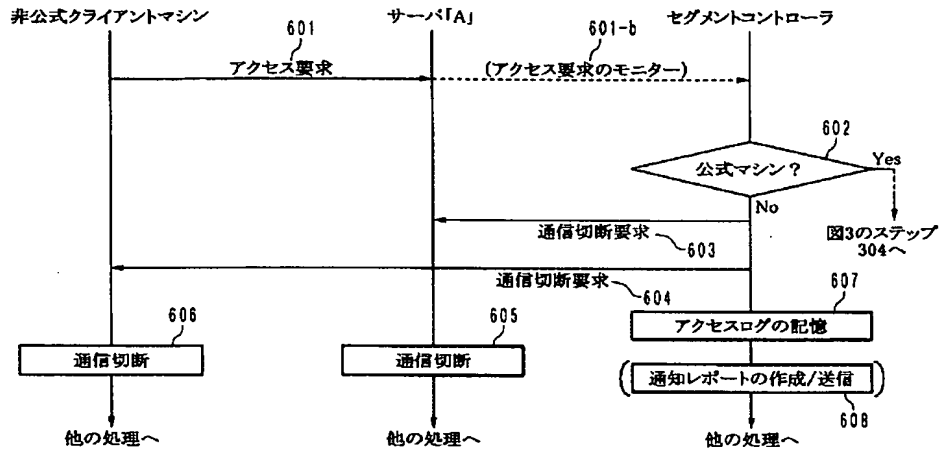
【図5】

【図5】



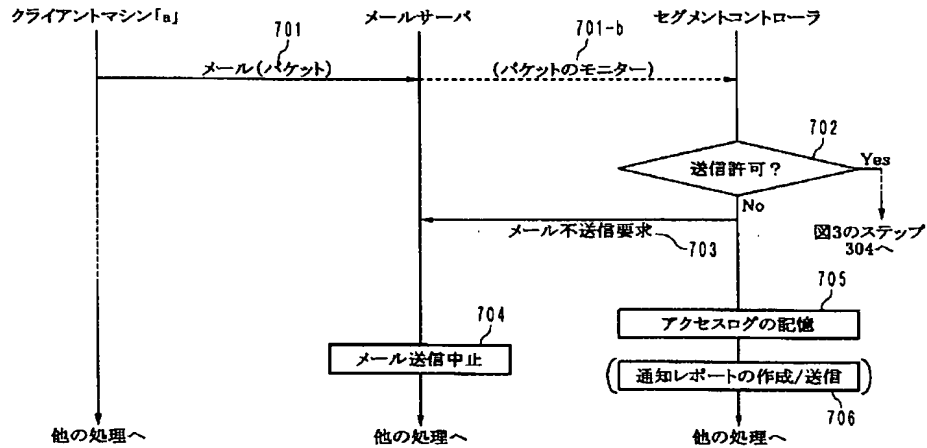
【図6】

【図6】



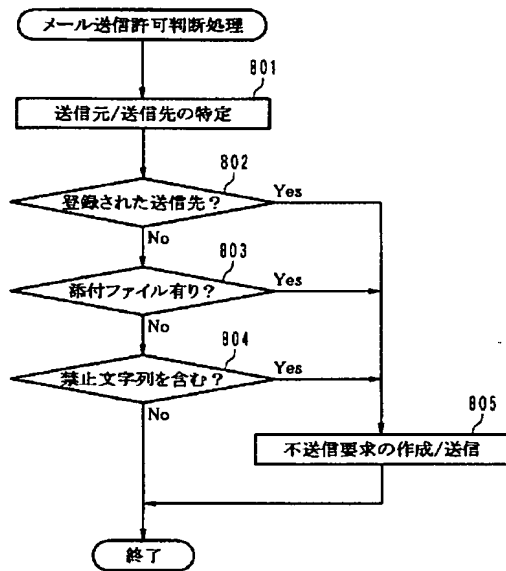
【図7】

【図7】



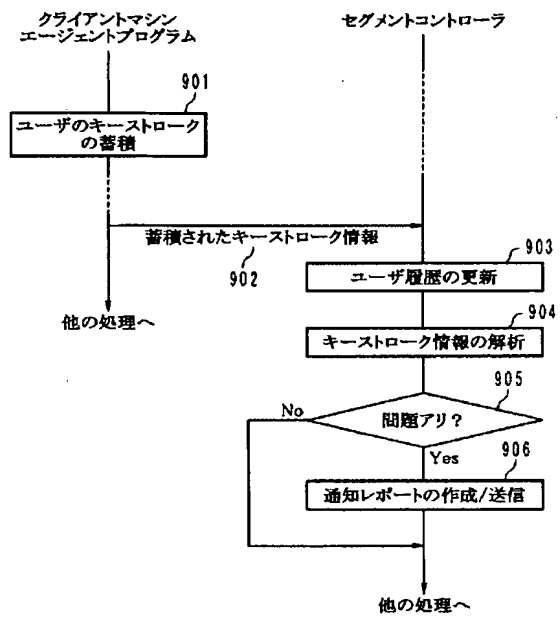
【図8】

【図8】



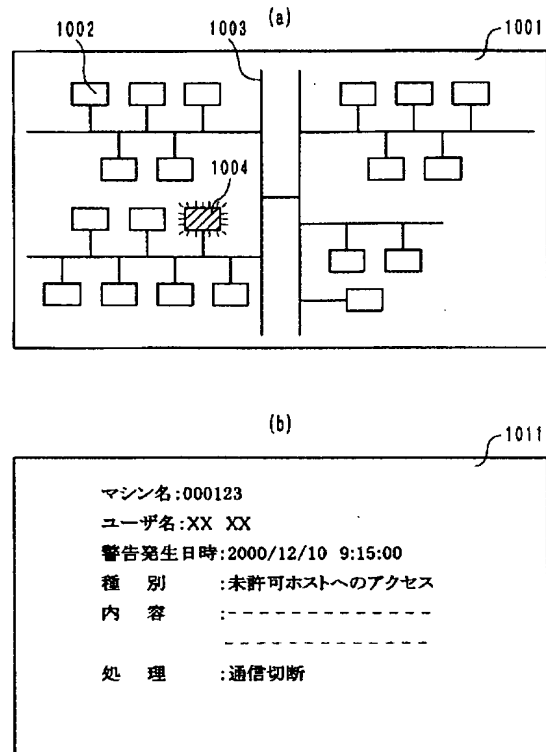
【図9】

【図9】



【図10】

【図10】




---

フロントページの続き

F ターム(参考) 5B089 GA31 GB02 JA31 KA17 KB13  
 KC52 KC54  
 5K033 AA08 CB08 DA01 DA05 DB19  
 EA06 EA07 EC04